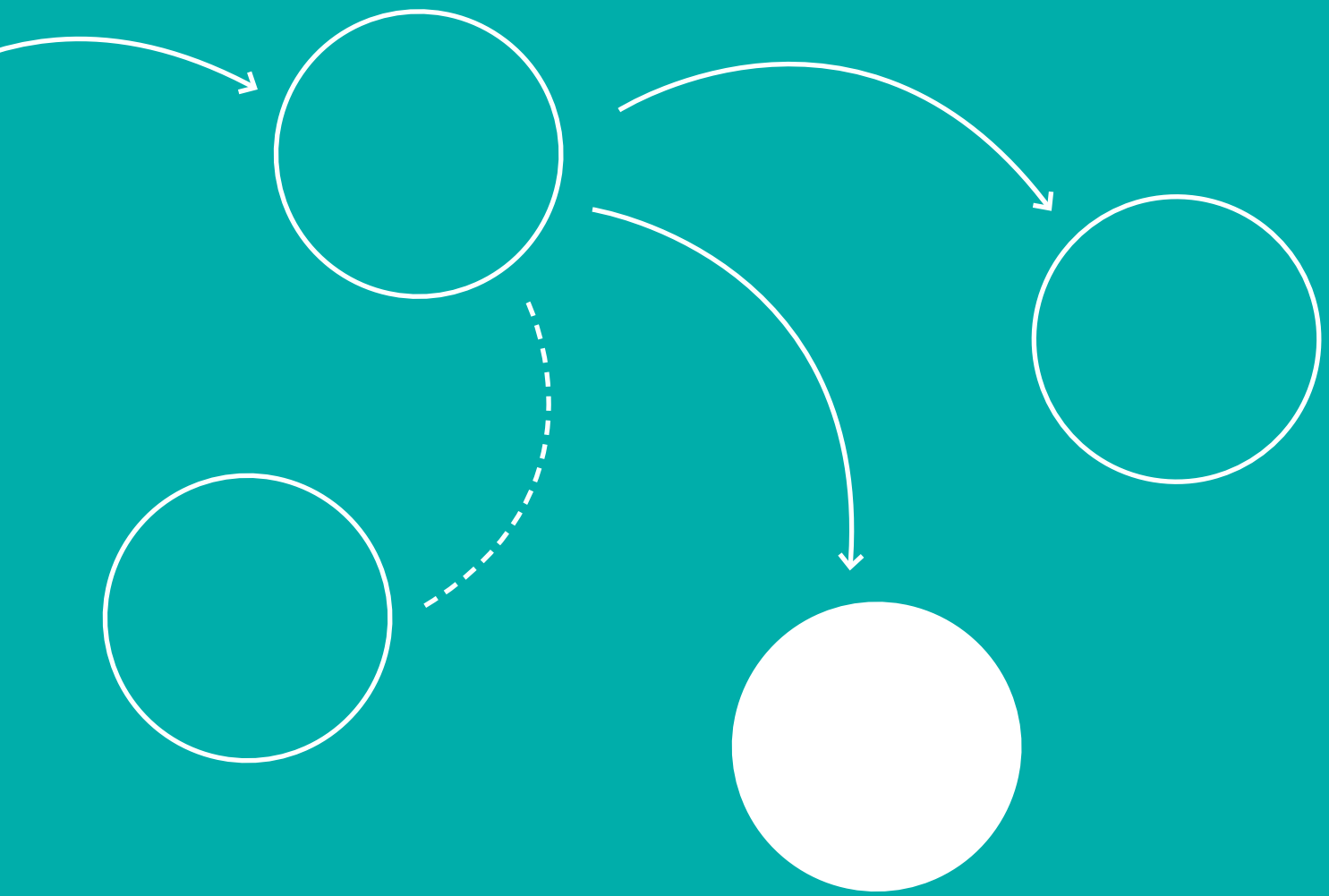
단말 이상행위 탐지 및 대응 솔루션

Genian EDR

v 2.X



Genians

Genian EDR

Overview

APT(지능형 지속 위협) 및 랜섬웨어 등의 보안 위협은 기하급수적으로 확산되고 있습니다.
이러한 악성코드를 활용한 공격은 단순한 보안 위협 수준을 넘어, 실질적이고 심각한 경제적 손실을 초래하고 있는 상황입니다. 날로 지능화되는 APT, 랜섬웨어 등은 전통적인 보안솔루션을 통해 탐지하고 대응하기 어려운 것이 현실입니다. 운영 중인 다양한 보안솔루션으로도 찾기 어려운 내부 이상 행위 및 침해 사고를 탐지하고 발생한 보안 위협에 빠르게 대응할 수 있는 단말 기반 지능형 위협 대응 솔루션이 필요합니다.

'지니안 EDR(Genian EDR)'은 단말에 대한 지속적인 모니터링 및 정보 수집을 통해 위협의 탐지 및 분석, 대응을 제공하는 단말 이상행위 탐지 및 대응(EDR: Endpoint Detection&Response) 솔루션입니다.

악성코드 및 이상 행위를 최신 침해 사고 지표(IOC)와 머신 러닝(ML) 행위 기반 엔진(XBA)을 활용해 신속하게 탐지하여 APT, 랜섬웨어 등의 공격을 실행단계에서 차단할 수 있습니다.

1. 단말 행위 모니터링/수집

- File, Module, Process, Network, Registry 정보
- 사용자 및 단말에서 발생하는 이상 행위
- 외부 저장매체의 파일 정보
- 윈도우 이벤트 수집(옵션)
- 다양한 대시보드 제공

2. 위협의 탐지

- 침해사고지표(IOC*) 기반의 알려진 위협 탐지
- 머신러닝(ML)기반의 알려지지 않은 위협 탐지
- 행위 기반의 File-less 위협 탐지
- 야라(YARA)를 이용한 사용자 설정 기반의 심층조사

3. 위협의 대응

- 탐지된 위협 대상의 고지, 종료, 삭제, 고립, 네트워크 격리
- 알려진 위협 사전 대응
- 분석 후 대응(대응 시 동일 이벤트 자동 대응)
- 샌드박스, SIEM 등 기존 보안 솔루션 연동

4. 탐지 위협의 조사/분석

- 탐지된 위협의 상세 정보 제공, 의심 파일 수집
- 통합 검색 및 연관 검색
- 이벤트 타임라인 및 연관 분석(Chain of Event)
- Ecosystem(평판 서비스) 제공

* IOC: Indicators of Compromise, 악성코드 및 접속 C&C 등 침해 사고의 흔적들에 대한 정형화된 데이터

적응형 위협 대응 프로세스

위협으로부터 사용자와 단말을 보호하는 '예방 – 탐지 – 분석 – 대응' 프로세스 구축이 가능하며 NAC(Network Access Control)와 협업하여 효율적으로 위협에 대응할 수 있습니다.

진행 전(Pre)

사전 예방 Prevention

- BYOD
- 인증/식별(단말, 사용자)
- 방문자 관리(Guest)
- 필수 S/W 설치 등

Genian NAC

진행 중(On)

조사/분석 Detection

- 잠재 위협/이상 행위
- 악성코드 전달 및 확산
- 공격자 명령 수행
- 알려진/알려지지 않은 위협

Genian EDR

진행 후(Post)

확산/재발 방지 Response

- 즉시 조치
- 위협 확산 방지
- 위협 제거
- 위협 예방

적응형 위협 대응

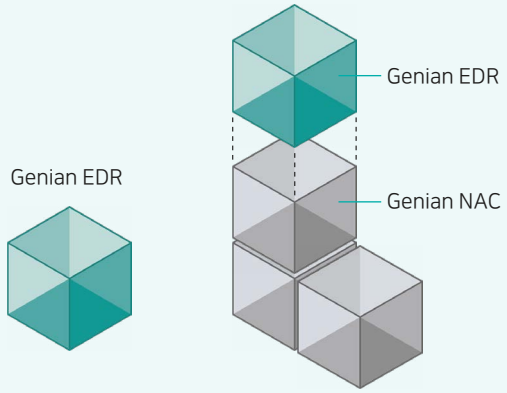
Key Features

에이전트 설치 및 운용

에이전트는 단독으로 설치/운영이 되며, Genian NAC 사용 환경에서는 에이전트가 통합되어 배포 시 '관리자 부담'과 '사용자 충격'을 최소화합니다.

단독/통합 에이전트 제공

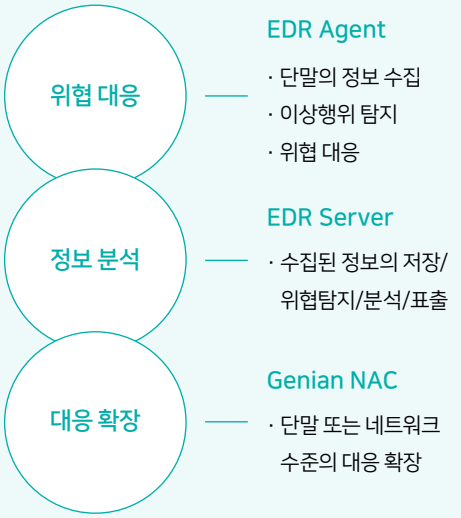
- NAC없는 환경에서 단독으로 설치/운영
- NAC 환경에서는 통합되어 추가 에이전트 설치 불필요
- 에이전트 설치/배포/운용 등 도입에 따른 부담 제로
- 인사정보(DB), 기존 단말 보안정책 등 주요기능 승계(NAC 사용 시)



단독 에이전트 통합 에이전트

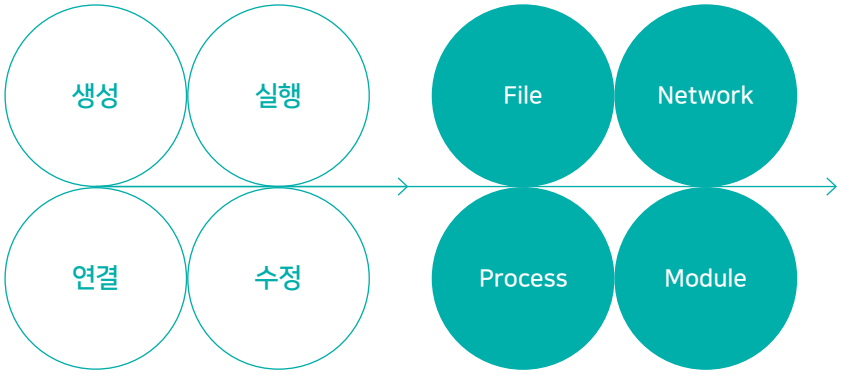
단말 부하를 최소화한 탐지 방식

- PC에 설치된 모듈을 통해 각종 정보 수집 후 서버에 전송
- 분석/탐지는 서버에서 이루어지며 사용자 PC 부하 최소화



단말 행위 모니터링

단말에서 발생하는 주요 행위를 모니터링하고 실시간 저장 후 분석합니다. 이를 통해 지능형 위협 등을 사전에 탐지/예방하고, 사후 감사 증적(Audit)이 가능합니다.



사용자, 단말의 행위 분석 및 이상행위(Anomaly) 탐지

APT, 랜섬웨어 등 지능형 위협의 탐지

탐지된 위협 및 이상행위 대응(Response)

침해 사고 및 이상행위의 감사 증적(Audit)

Key Features

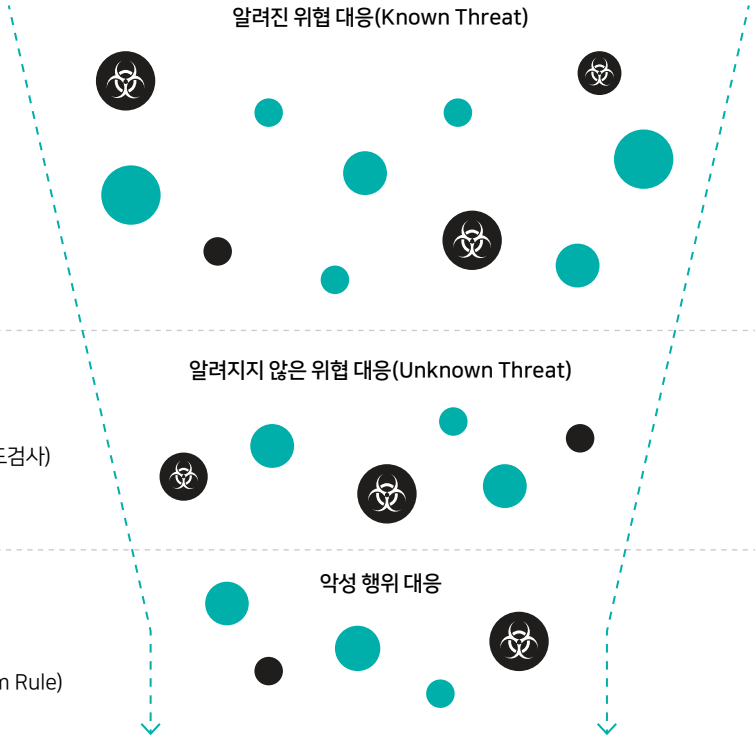
위협(Threat) 탐지

IOC(침해 사고 지표), 머신 러닝, YARA를 이용하여 단계별로 위협을 탐지하며 최고 수준의 정탐률(악성파일+정상파일 탐지)을 제공합니다. XBA(행위 기반 엔진)을 통해 File-less를 포함한 다양한 형태의 악성행위를 탐지합니다.

IOC(침해 사고 지표)
- Malware IOC
- Goodware DB
- C2 IP

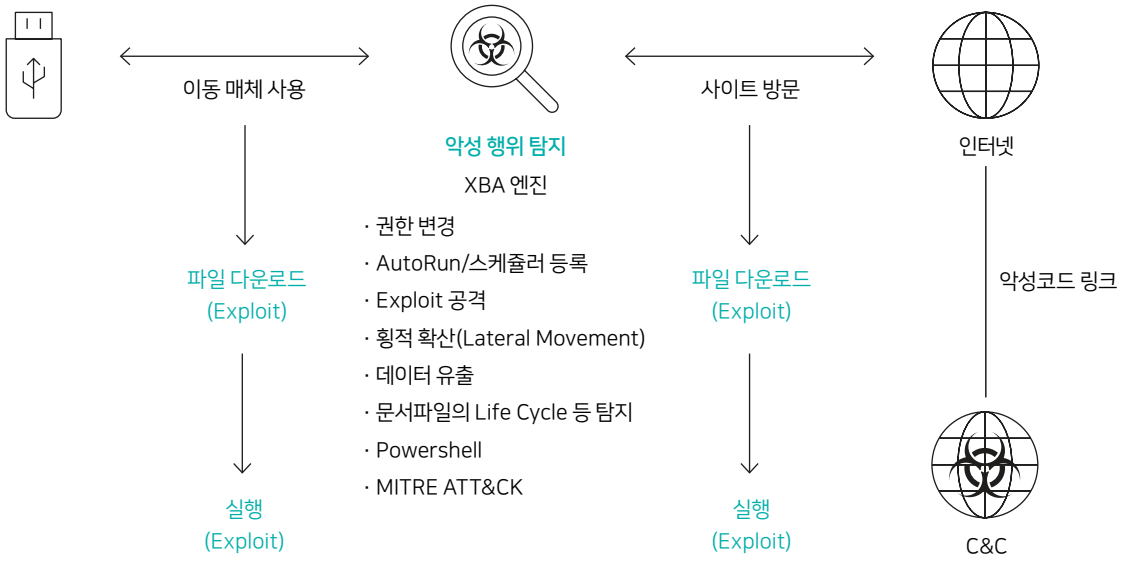
ML+YARA(머신러닝+야라)
- Static Analysis
- YARA(규칙기반 악성코드검사)

XBA(행위 기반 엔진)
- 행위기반 탐지 Rule
- File-less
- 관리자 정의정책(Custom Rule)



이상행위 탐지

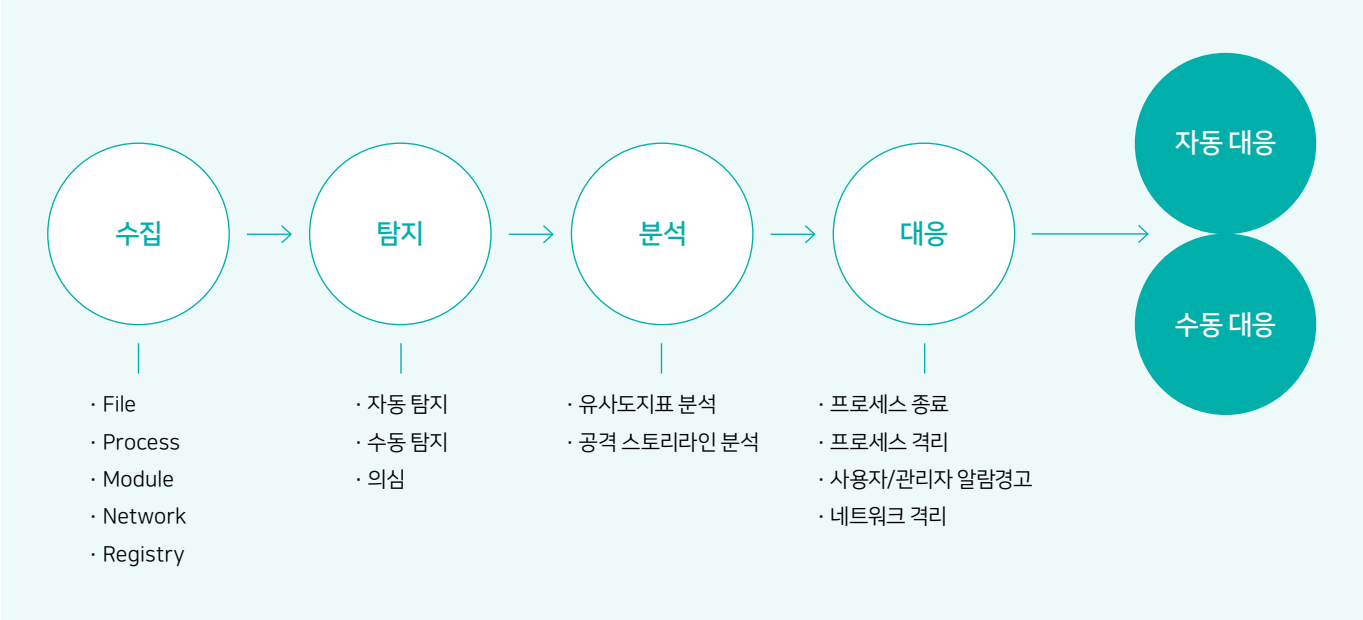
사용자 행위 및 단말의 이벤트를 감시하여 이상행위를 탐지합니다. 이상행위 여부 분석 후 위협의 조기 발견 및 IOC 등으로 대응하기 어려운 이상 행위를 탐지할 수 있습니다.



Product Function

위협 대응

단말에서 위협이 탐지되는 경우 위협의 '심각성, 확산성, 위험성' 등을 고려하여 에이전트에서 네트워크 격리, 파일 삭제, 프로세스 종료, 사용자 알림 등의 대응을 합니다. 정책(Policy) 기반으로 관리자 개입 없이 즉시 작용하므로 확산 방지 등 초동 대응이 가능합니다.



Genian EDR 위협 대응 프로세스

탐지 위협의 조사

위협의 탐지와 동시에 조치의 대상이 누구인지 '사용자, 부서, ID' 등을 정확하게 알 수 있으며 ReversingLabs, VirusTotal 등의 외부 인텔리전스(CTI) 조회를 통해 탐지된 위협의 상세정보 확인이 가능합니다.

탐지 기본 정보

일반 정보	탐지 시각 | 위협 분류 | 위협 ID
사용자 정보	부서 | 사용자 이름 | ID
단말 정보	IP | MAC | Hostname | OS | ID
파일 정보	이름 | 경로 | 크기 | 해쉬값

정적 분석(Static Analysis) 정보

제품 정보	버전 | 카피라이트 | 이름 등
코드사인	코드사인(Signature Verification) 정보
PE 정보	섹션 | 타입 | 체크섬 | 엔트리포인트 등
문자열 정보	유형 | 종류 | 문자열 | 위치 등

동적 분석(Dynamic Analysis) 정보

환경 정보	OS | 설치된 프로그램 | 시간 등
행위 요약	프로세스 경로 | 행위 내용 등
시스템 행위	레지스트리, 파일, 동적링크(dll) 등 행위의 발생 시간, 값, 결과 등
네트워크 행위	Protocol | Appl. | Port | Count 등

연관 분석(Chain of Event) 정보

연관 관계	파일 및 프로세스 실행 | 호출 | 연결 등 행위 연관 관계 | 유입경로
상세 정보	파일 및 프로세스 크기 | Path | IP | Hash | ID 등
수행 명령어	파일 실행 위치 | 옵션 값 등

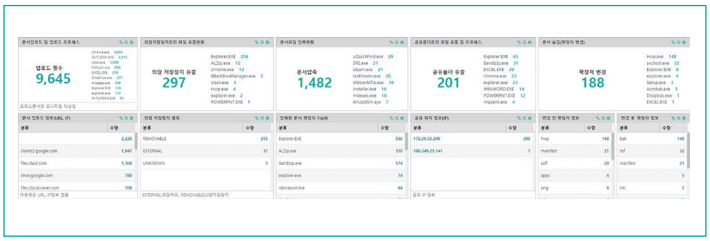
Product Function

Endpoint Discovery

위협 탐지를 위해 실시간으로 수집한 로그는 다시 활용하여 기존에 알 수 없었던 단말에서 행해지는 상황을 파악할 수 있습니다. 문서 유출(업로드), 네트워크 접속 현황, AP접속 현황, 외장저장장치 사용, 메신저, 클라우드 서비스 사용자, DNS 변경 외 다수

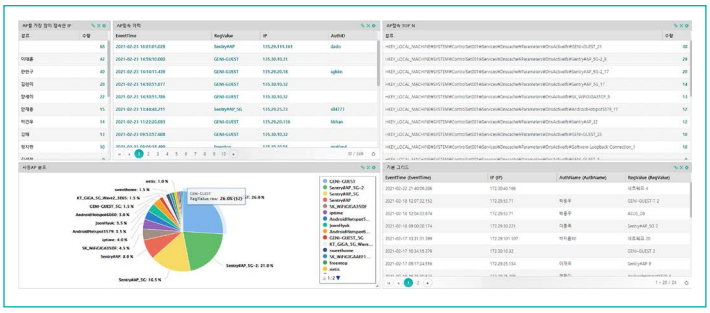
문서 유출 모니터링

- 문서 업로드(Web, SNS 등)
- 외장 저장장치(USB, HDD 등) 복사/이동
- 문서 압축
- 확장자 변경 등



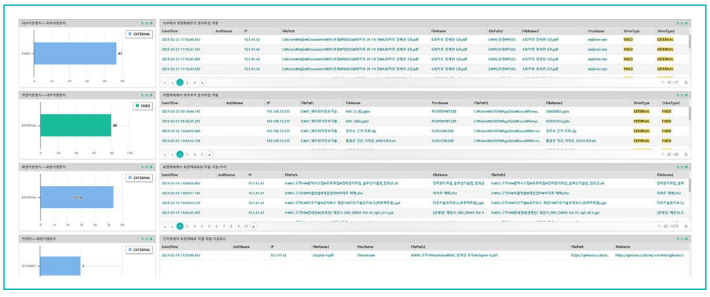
네트워크 접속 현황

- 단말의 유/무선 접속 현황
- SoftAP(테더링) 접속
- 외부 AP 접속
- 원격데스크탑/원격터미널 접속
- Putty, Telnet, FTP 등 접속 등



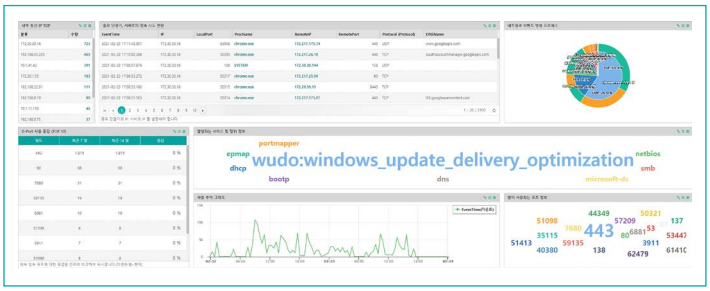
외장 저장장치 세부 사용 현황

- 외장 저장장치로 복사/이동에 대한 세부 내용
- PC → 외장 저장장치로 복사/이동
- 외장 저장장치 → PC로 복사/이동
- 외장 → 외장 저장장치로 복사/이동
- Internet → 외장 저장장치로 다운로드



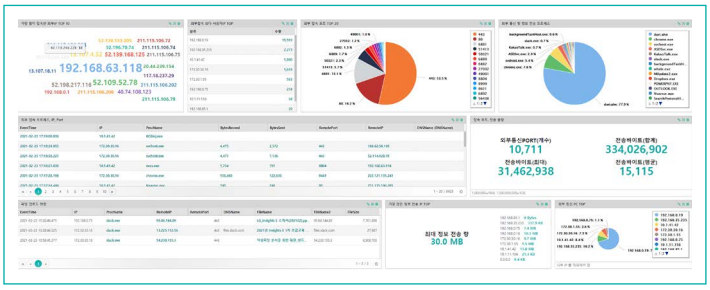
네트워크 이상 분석

- 네트워크 추이 현황(전주/금주 등)
- 오픈 포트 및 서비스 종류
- 네트워크 사용 프로세스 목록
- 특정 단말(관리자 PC 등)로의 접속 현황 등



특정 외부 IP 통신 분석

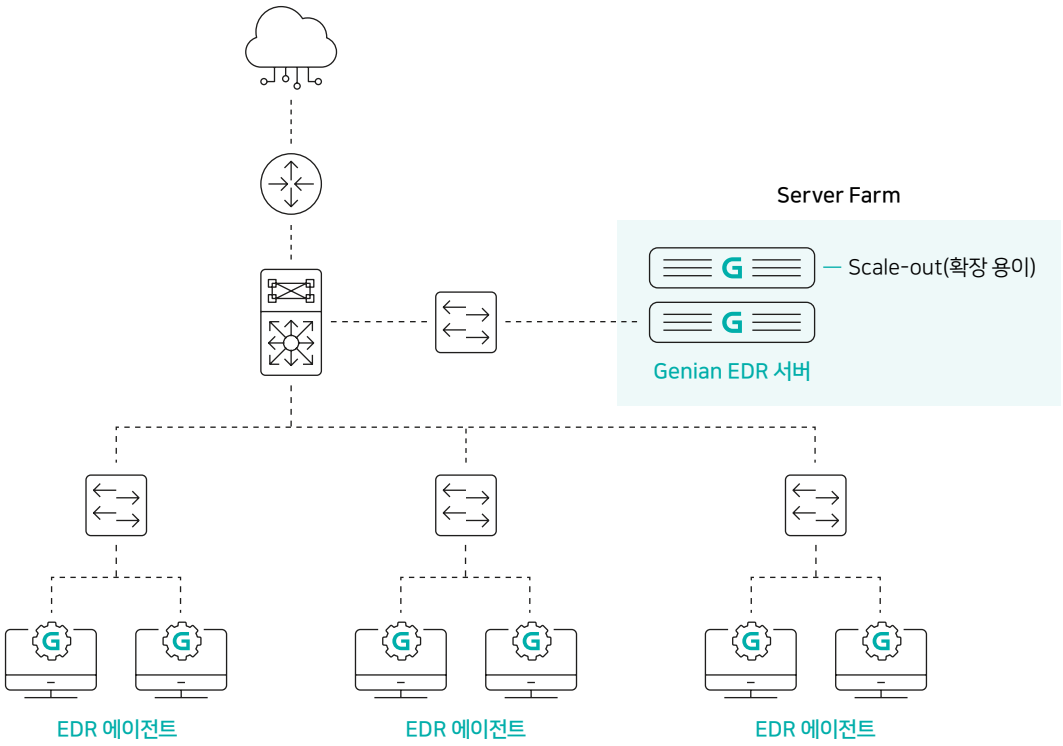
- 오픈 포트
- 세션을 통해 전송한 Byte 수
- 외부 IP 접속 프로세스 등



Operating Mode

구성

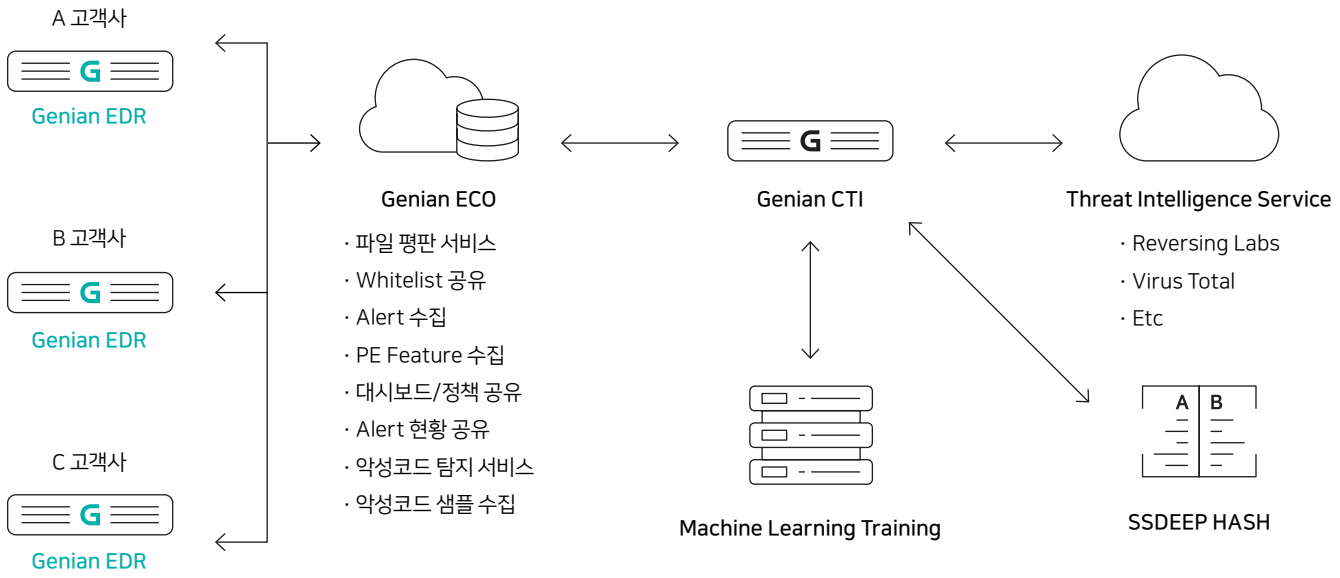
Genian EDR 서버와 EDR 에이전트의 간단한 구성입니다. Scale-Out 기능을 제공하여 쉽게 확장 할 수 있습니다.



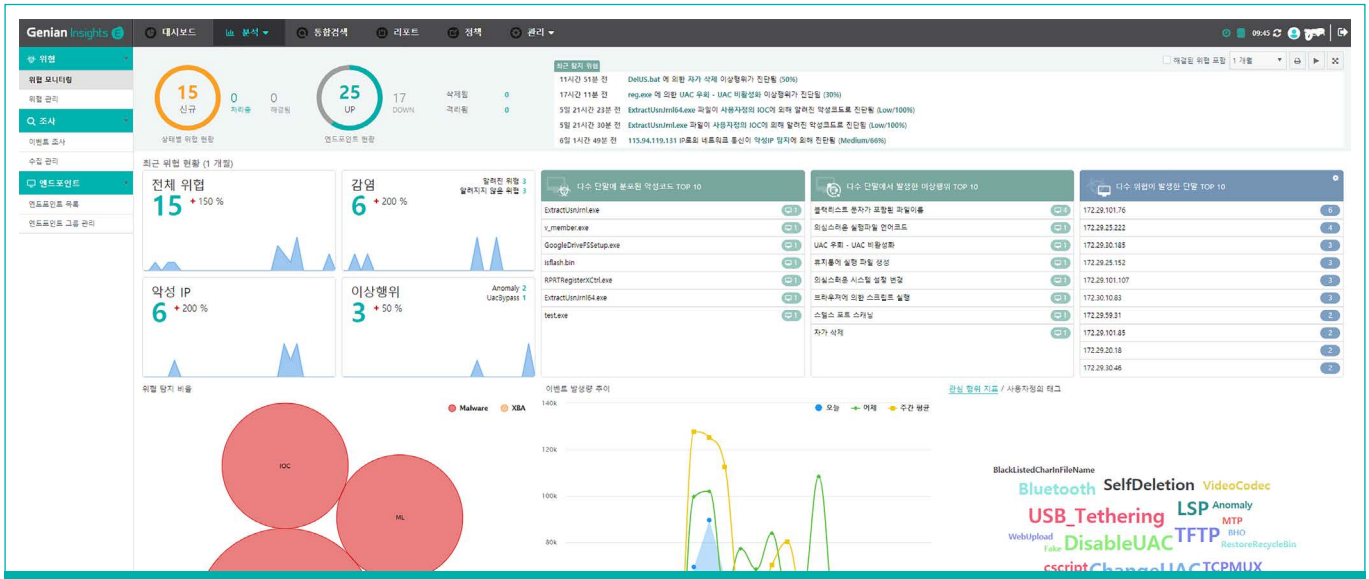
* Genian NAC 사용 시, NAC Agent에 EDR 플러그인(모듈) 형태의 간단한 배포와 인증정보 자동 연동 기능 제공

Ecosystem

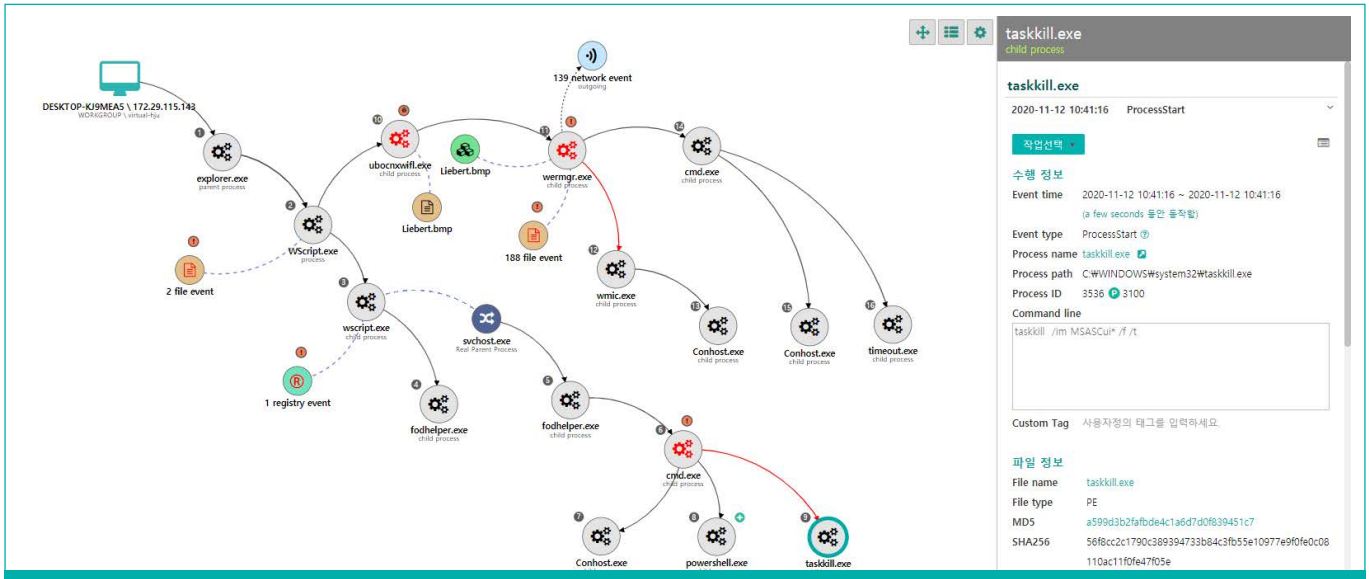
고객사에서 수집된 위협 정보를 Ecosystem으로 보내 위협에 대한 분석 결과(평판 서비스)를 제공하며 고객사에서 수집된 위협과 예외 처리된 데이터를 확인 및 가공하여 Genian EDR를 사용하는 고객사에 재 배포합니다. (파일이 아닌 파일의 HASH, Feature 정보를 전송합니다.)



Adminstrator UI



위협 모니터링



공격 스토리 라인

Genian EDR 서버

- CPU : Intel 2.1G (8C16T) * 1
- Mem : 64GB
- HDD/SSD : 10TB/1.92TB
- Port : 1G/10G * 2
- 2U/Single Power

- CPU : Intel 2.1G (8C16T) * 2
- Mem : 128GB
- HDD/SSD : 10TB/3.84TB
- Port : 1G/10G * 2
- 2U/Dual Power

EDR 에이전트

- Windows 7/10/11 지원
- 단독 에이전트 설치
- Genian NAC 사용 시 에이전트 모듈로 추가
- 메모리 점유 9~12M
- 일 평균 10M 수준의 정보 수집*

* 측정 평균치이며, 업무 환경에 따라 달라질 수 있습니다.

14058 경기도 안양시 동안구 벌말로 66 평촌역 하이필드 지식산업센터 A동 12층
기술지원 : 1600-9750 (평일 오전 9시~오후 9시) / 도입문의 : sales@genians.com

Genians